Abstract

A biometric based security system provides best on both authentication and confidentiality for public shared secret information. Enormous numbers of papers have been published by the researchers in this field. The generation of prime numbers plays the most important role in the public-key schemes, essentially as a major primitive needed for the creation of key pairs or as a computation stage appearing during various cryptographic setups. Most of the researchers have been made strong mathematical studies on primality testing and an observed progressive increase of cryptographic usages, prime number generation algorithms. Still not quite investigated and most of the real-life implementations are providing poor performance. Most of the common prime number generators typically output n-bit prime in heuristic average complexity.

References

1. A.O.L. Atkin, D.J. Bernstein, Prime sieves using binary quadratic forms, Math. Comp. 73


9. G. H. Hardy and J. E. Littlewood. “Some problems of ‘partitio numerorum’: III. on the expression of a number as a sum of primes”, 44, pp. 1–70, 1922


33. H.C. Pocklington. The determination of the prime or composite nature of large numbers by Fermat's theorem. Proc. of the Cambridge Philosophical Society, vol. 18, pp. 29-30, 1914
40. http://biometrics.idealtest.org/dbDetailForUser.do?id=7
Index Terms

Computer Science

Algorithms

Keywords

Biometric Identity, Prime numbers, Public Key Infrastructure (PKI).